IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

Diana K. Smith, Edward L. Scherer, and Adrian Michael Azocar; Individually, and on behalf of all others similarly situated, Plaintiffs,	)	**Civil Action File No.**
v.	)	
Equifax Inc. and Equifax Information Services LLC Defendants.	)	**Jury Trial Demanded**

ORIGINAL CLASS ACTION COMPLAINT

CLASS PLAINTIFFS, Diana K. Smith, Edward L. Scherer and Adrian Michael Azocar ("Plaintiffs"), by and through their attorneys, and on behalf of themselves, the Nationwide Class, each Statewide Sub-Class, and in the public interest, bring this class action complaint against Equifax Inc. and Equifax Information Services LLC (collectively, "Defendants" or "Equifax"). Plaintiffs would respectfully show the Honorable Court as follows:

I. INTRODUCTION

1. Class Plaintiffs bring this civil action on behalf of themselves and all others similarly situated to redress Defendants' enormous failure to adequately safeguard personal identifying information and related data.

2. This action arises from what is one of the largest and most horrific data security breaches ever to occur in the United States, affecting approximately 143,000,000 individuals – effectively 50% of the U.S. population.

3. As a result of this breach, Plaintiffs and these millions of individuals whose sensitive personal data was made accessible to the dark web now face eminent and substantial risk of further injury from identity theft, credit and reputational harm, false tax claims, or even extortion. The sheer magnitude of the invasion of privacy of millions of individuals is mind boggling, especially in light of the fact that the security breach could easily have been prevented months ago.

4. Also as a result of the staggering array of personal information that has been compromised, Plaintiffs and the Putative Class members (i.e., class members of all classes proposed herein) will have to remain vigilant for the rest of their lives to combat potential identity theft arising from the critical (and in some instances, irreplaceable) data that are now in the hands of cyber criminals, who may use such data for any purpose, at any point, in perpetuity. Despite all best efforts of Plaintiffs and Putative Class members, or any other third party to scrub these data from the World Wide Web, they are potentially forever recoverable by anyone who wishes to find such data.

5. The potential repercussions for consumers are egregious. Privacy researchers and fraud analysts have called this attack "as bad as it gets." "On a scale of 1 to 10 in terms of risk to consumers," it is a 10.[1]

6. Class Plaintiffs bring this FRCP 23 class action pursuant to, and claim all available remedies under, the Fair Credit Reporting Act (15 U.S.C. § 1681, *et seq.* ("FCRA")), the data breach statutes and consumer protection statutes of the various states and jurisdictions enumerated herein (including the Texas Deceptive Trade Practices Act (DTPA)), negligence and unjust enrichment.

---

[1] https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html

II.
JURISDICTION AND VENUE

7. Plaintiffs, on behalf of themselves and the Putative Classes, bring this action pursuant to a federal statute, the Fair Credit Reporting Act, 15 U.S.C. § 1681, *et seq*.

8. Further, this Court has jurisdiction under 28 U.S.C. § 1332 because there are over 100 Class Members, the amount in controversy exceeds $5 million exclusive of interest and costs, and this is a class action in which many members of the proposed classes, on the one hand, and Defendant, on the other, are citizens of different states.

9. The Southern District of Texas has personal jurisdiction over Defendants because Defendants conduct business in Texas and in this district; Defendants advertise in a variety of media throughout the United States, including Texas; and many of the acts complained of and giving rise to the claims alleged herein occurred in Texas in this district. Defendants intentionally avail themselves of the markets within this state to render the exercise of jurisdiction by this Court just and proper.

10. The Court has supplemental jurisdiction over state law under 28 U.S.C. § 1367. Any state law claims alleged now, or in the future, are so related in this action within such original jurisdiction that they form part of the same case or controversy under Article III of the United States Constitution.

11. Venue is proper in the United States District Court for the Southern District of Texas under 28 U.S.C. § 1391. Plaintiffs reside in this District and their claims arise, in substantial part, in this District.

III.
THE PARTIES

12. Individual and representative Plaintiffs Diana K. Smith, Edward L. Scherer and Adrian Michael Azocar each reside in Harris County, Texas. Plaintiffs Smith, Scherer and Azocar are members of each of the Putative Classes. Each named Plaintiff is an individual consumer who resided in Houston, Texas during the period relevant to this litigation. Each Plaintiff engaged, or authorized the engagement of, Equifax at various times over the years. As a result, Equifax has possessed each Plaintiff's financial history, including a social security number, birthdate, driver's license number, personal addresses, telephone numbers, and other sensitive personally identifying information ("PII"). Each Plaintiff was a victim of Equifax's security breach, which has placed each Plaintiff at substantial, immediate and eminent risk of harm, harm that was readily preventable.

13. Defendant Equifax Inc. is a multibillion dollar corporation formed under the laws of the state of Delaware with its corporate headquarters at 1550 Peachtree Street NE, Atlanta, Georgia 30309. Equifax Inc. is a "Consumer Reporting Agency" (or "CRA") under 15 U.S.C. 1681a(f). Further, Equifax Inc. is a "Consumer Reporting Agency that Compiles and Maintains Files on Consumers on a Nationwide Basis" under 15 U.S.C. 1681a(p). This Defendant provides credit information services to millions of businesses, governmental units, and consumers across the globe. The company organizes and analyzes data on more than 820 million consumers and more than 91 million businesses worldwide, and its databases hold employee data submitted by more than 7,100 employers. Equifax Inc. operates through various subsidiaries and agents, each of which entities acted as agents of Equifax Inc., or in the alternative, in concert with Equifax Inc.

14. Defendant Equifax Information Services LLC operates as a subsidiary of Equifax Inc. and collects and reports consumer financial information to financial institutions. Equifax

Information Services LLC is a limited liability company incorporated in Georgia with its principal place of business at 1550 Peachtree Street NE, Atlanta, Georgia 30309. This Defendant is a CRA pursuant to 15 U.S.C. §§ 1681a(f) and 1681a(p).

15. Whenever alleged herein that Defendants committed any act or omission, it is meant that Defendants' officers, directors, vice-principals, agents, servants, or employees committed such act or omission and that at the time the act or omission was committed, it was committed with full authorization, ratification or approval of Defendants or was done in the routine normal course and scope of employment of Defendants' officers, directors, vice-principals, agents, servants, or employees.

IV.
FACTUAL ALLEGATIONS

16. On September 7, 2017, Defendants publicly disclosed a massive data security breach that affected approximately 143,000,000 American consumers, 400,000 U.K. consumers and 100,000 Canadian consumers.

17. Defendants state the cyberattack was carried out from mid-May to July 2017.

18. Defendants further state they discovered the cyberattack on July 29, 2017.

19. Even though Defendants discovered the cyberattack on July 29, 2017, and despite the breadth and severity of the release of PII, Defendants waited approximately six weeks before publicly announcing the breach. From a consumer's standpoint, this delay of weeks was unreasonable because from day one after the breach, criminals were using the PII to incur severe damage to the affected consumers. In essence, Plaintiffs and the Putative Class members were sitting ducks. They had no knowledge of the breach, and thus no one was able to mitigate damages as soon as possible. Equifax had a duty to inform consumers of the breach immediately so that the consumers could have taken steps to prevent or lessen the damages that will follow.

20. Equifax's delay in informing the consumers is the direct and proximate cause for the immediate, eminent and severe risk of harm that will come to them, and in some cases has already come to them in varying forms of their worst nightmares.

21. Not surprisingly, the Department of Justice, along with the FBI, has opened a criminal investigation into whether three top Equifax officials violated insider trading laws when they sold company stock before making disclosure of the cyberattack to the public on September 7, 2017. Federal prosecutors are examining the nearly $1.8 million in sales of Equifax stock by Chief Financial Officer John Gamble, Joseph Loughran (president of the Equifax's U.S. Information Solutions division), and Rodolfo Ploder (president of the Equifax's Workforce Solutions Unit). Regulatory filings show the executives' stock sales were conducted in the days after Equifax discovered the security breach, and long before the company notified investors and the public.

22. Defendants admit their U.S. website application had a security "vulnerability" that allowed third parties to access a vast amount of individual PII. According to the Apache Foundation, which oversees the widely-used open source software, **"The Equifax data compromise was due to (Equifax's) failure to install the security updates provided in a timely manner"**.

23. Equifax admitted that the criminals who gained access to its customer data exploited a website application vulnerability known as Apache Struts CVE-2017-5638.

24. Cybersecurity professionals who lend their free services to the project of open-source software — code that's shared by major corporations and that's tested and modified by developers working at hundreds of firms — had shared their discovery with the industry group, making the risk and fix known to any company using the software. Modifications were made on

March 10, 2017, according to the National Vulnerability Database. But two months later, hackers took advantage of the vulnerability to enter Equifax's systems (Equifax states the unauthorized access began in mid-May).

25. As a result of Defendants' actions / inactions, the social security numbers, birthdates, driver's license numbers, personal addresses, telephone numbers, and other sensitive personally identifying information of millions of U.S., U.K. and Canadian consumers were released. Hackers also gained access to credit card numbers for approximately 209,000 consumers, as well as dispute records containing the personal identifying information of roughly 182,000 consumers.

26. It goes without saying that none of the individuals, including Plaintiffs and Putative Class members, whose personal information was compromised authorized such access or disclosure by the Defendants.

27. Defendants themselves state that the data was accessed by – and therefore presumably is in the hands of – "criminals." These criminals had one purpose for stealing millions of individuals' sensitive data – to steal their money, credit, and identity, and to commit other damaging acts. The very real and grave impact of their crimes have caused, and will continue to cause damages to Plaintiffs and Putative Class members for years to come.

28. Defendants purport to be sophisticated companies with "industry expertise" in handling "trusted unique data", including the highly sensitive personal information of individual consumers like Plaintiffs and the Putative Class members.

29. Despite such representations, Defendants have been sued, investigated and fined multiple times in recent years for fundamental flaws in their systems that store and handle PII.

30. More than a month after the breach, Equifax established a website that allows U.S.

consumers to determine whether their data may have been compromised and to enroll in free credit monitoring.

31. The website Equifax set up and directed consumers to use to check whether their PII had been compromised was itself fraught with security risks. The site has a flawed Transport Layer Security implementation, and runs on free blogging software unsuitable for secure applications.

32. The site also seeks from consumers their last name, as well as the last six digits of the social security numbers, without any assurance that the information would be secure. It fails to warn consumers to use a secure computer or encrypted network to transmit such sensitive information.

33. In order to use the TrustedID free credit monitoring, the site also asks consumers to waive certain legal rights via an inconspicuous arbitration clause.

34. Upon information and belief, the wrongful acts and decisions made by the Defendants leading to this data breach occurred nationwide and in this District.

35. Equifax owed a duty to Plaintiffs and the Putative Classes, who entrusted Defendants with their private information, to use reasonable care to protect their PII from unauthorized access by third parties and to detect and stop data breaches, to comply with laws implemented to preserve the privacy of this information, and to notify them promptly if their information was disclosed to an unauthorized third party.

36. Equifax knew or should have known that its failure to meet this duty would cause substantial harm to Plaintiffs and the Putative Classes, including serious risks of credit harm and identity theft for years to come.

37. Equifax was aware that the PII collected, maintained and stored in their information technology systems is highly sensitive, susceptible to attack, and could be used for wrongful purposes by third parties, such as identity theft and fraud. It is well known and the subject of many media reports that PII is highly coveted and a frequent target of hackers.

38. Prior to May 2017, Equifax had experienced at least three major cybersecurity incidents in which consumers' personal information was compromised and accessed by unauthorized third parties.

39. Despite the frequent public announcements of data breaches of corporate entities, including Experian and Equifax itself, Equifax maintained an insufficient and inadequate system to protect the PII of Plaintiffs and Putative Class members, in breach of its duties to Plaintiffs and the Putative Classes. Given Equifax's history of cyberattacks and its reputation as an industry leader in data breach security, Equifax could have and should have invested more money and resources into ensuring the security of its data.

40. The Equifax data breach was a direct and proximate result of Equifax's failure to properly safeguard and protect Plaintiffs' and Putative Class members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Equifax's failure to establish and implement appropriate safeguards to ensure the security and confidentiality of Plaintiffs' and Putative Class members' PII to protect against reasonably foreseeable threats to the security or integrity of such information.

41. At all relevant times, Equifax knew, or reasonably should have known, of the importance of safeguarding PII and of the foreseeable consequences if its data security system was breached, including, specifically, the significant costs that would be imposed on individuals as a result of a breach.

42. As a direct, proximate, and foreseeable result of Equifax's failure to meet its duty of care, including by failing to maintain adequate security measures and failing to provide adequate notice of the data breach, Plaintiff and the Putative Classes have suffered and will continue to suffer substantial harm, including inconvenience, distress, injury to their rights to the privacy of their information, increased risk of fraud, identity theft, and financial harm, the costs of monitoring their credit to detect incidences of this, and other losses consistent with the access of their PII by unauthorized sources.

43. Armed with the stolen information, unauthorized third parties now possess keys that unlock consumers' medical histories, bank accounts, employee accounts, and more. Abuse of sensitive credit and personal information can result in considerable harm to victims of security breaches. Criminals can take out loans, mortgage property, open financial accounts and credit cards in a victim's name, obtain government benefits, file fraudulent tax returns, obtain medical services, and provide false information to police during an arrest, all under the victim's name. Furthermore, this valuable information can also be sold to others with similar nefarious intentions.

44. As a direct and proximate result of Equifax wrongful actions and inaction and the resulting data breach, Plaintiffs and Putative Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time that they otherwise would have dedicated to other life demands such as work and effort to mitigate the actual and potential impact of the data breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports. This time has been lost forever and cannot be recaptured. In all manners of life in this country, time has

constantly been recognized as compensable, for many consumers it is the way they are compensated, and even if retired from the work force, consumers should be free of having to deal with the consequences of a credit reporting agency's slippage, as is the case here.

45. A breach of this scale requires Plaintiffs and Putative Class members to incur the burden of scrupulously monitoring their financial accounts and credit histories to protect themselves against identity theft and other fraud and will spend time and incur out-of-pocket expenses to protect against such theft. This includes obtaining credit reports, enrolling in credit monitoring services, freezing lines of credit, and more. Where identity theft is detected, Plaintiffs and Putative Class members will incur the burden of correcting their financial records and attempting to correct fraud on their accounts, to the extent that that is even possible. Plaintiffs and Putative Class members will no doubt spend considerable effort and money for the rest of their lives on monitoring and responding to the repercussions of this cyberattack.

46. Equifax's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiffs' and Putative Class members' PII, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. theft of their personal and financial information;

b. unauthorized charges on their debit and credit card accounts;

c. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals and already misused via the sale through the dark web of Plaintiffs' and Putative Class members' information on the black market;

d. the untimely and inadequate notification of the data breach;

e. the improper disclosure of their PII;

f. loss of privacy;

g. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the data breach;

h. ascertainable losses in the form of deprivation of the value of their PII, for which there is a well-established national and international market;

i. ascertainable losses in the form of the loss of cash back or other benefits as a result of their inability to use certain accounts and cards affected by the data breach;

j. loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse credit notations; and,

k. the loss of productivity and value of their time spent to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all such issues resulting from the data breach.

47. Because Equifax has demonstrated an inability to prevent a breach or stop it from continuing even after being detected, Plaintiffs and members of the Putative Classes have an undeniable interest in insuring that their PII, which remains in Equifax's possession, is secure, remains secure, is properly and promptly destroyed and is not subject to further theft.

48. Clearly, the damages Plaintiffs and Putative Class members have suffered are not speculative. Rather, they have already occurred; they are concrete, real, material, non-imaginary, injuries-in-fact, tangible, quantifiable, and all other descriptors that take them out of the realm of non-justiciability in this Court. Such damages confer standing to each Plaintiff and Putative Class member under Article III of the U.S. Constitution.

V.
CLASS ACTION ALLEGATIONS

49. Plaintiffs bring this action pursuant to FRCP 23, seeking injunctive and monetary relief for Equifax's systematic failure to safeguard PII of each Plaintiff and each member of the Putative Classes defined herein. Each Plaintiff seeks relief in his or her individual capacity and as a representative of all others who are similarly situated.

Class Definitions:

50. The **Nationwide Class** is defined as all United States residents whose PII was made accessible in the data breach Equifax announced on September 7, 2017.

51. The **Statewide Sub-Classes** are defined as all residents of [name of State, District of Columbia, or U.S. Territory] whose PII was made accessible in the data breach Equifax announced on September 7, 2017.

52. Excluded from these classes are:

a. Any Judge or Magistrate Judge presiding over this action, and any involved Court personnel, and members of their families;

b. Defendants, Defendants' subsidiaries, parents, successors, predecessors, and any entity in which the Defendants or their parents have a controlling interest and their current and former employees;

c. Counsel for Plaintiffs and Defendants;

d. Persons who properly execute and file a timely request for exclusion from the Putative Classes;

e. The legal representatives, successors or assigns of any such excluded persons;

f. All persons who have previously had claims finally adjudicated or who have released their claims against the Defendants similar to those alleged herein; and,

g. Any individual who contributed to the unauthorized access to Defendants' database.

53. While the exact number and identities of the Putative Class members are unknown at this time, and can only be ascertained through appropriate discovery, upon information and belief, the classes are so numerous – over 143,000,000 – that joinder of all Putative Class members is impracticable.

54. This class action, along with multiple other cases, will likely be consolidated under the MDL rules found at 28 U.S.C. § 1407, *et seq.*

55. Questions of law and fact common to all Putative Class members predominate over questions affecting only individual members of the Putative Classes, including, without limitation:

a. Whether the Defendants owed a legal duty to the Putative Class members under federal and state law to protect their PII, provide timely notice of unauthorized access to this information, and provide meaningful and fair redress;

b. Whether Defendants breached this duty;

c. Whether Defendants acted wrongfully by improperly monitoring, storing and failing to properly safeguard consumers' PII;

d. Whether Defendants knew, or reasonably should have known, about the deficiencies in their data storage systems;

e. Whether Defendants willfully failed to design, employ and maintain a system adequate to protect consumers' PII;

f. Whether representations that Defendants made about the security of their systems were false or misleading;

g. Whether Defendants' actions and omissions violated applicable state consumer protection laws;

h. Whether Defendants' failures resulted in the breach at issue;

i. Whether Defendants failed to properly and timely notify each Plaintiff and each Putative Class member of the breach as soon as practical after it was discovered; and,

j. Whether each Plaintiff and each Putative Class member has been damaged and, if so, the appropriate relief.

56. Each Plaintiff's claims are typical of the claims of all Putative Class members because such claims arise from the Defendants' wrongful conduct, as alleged above, pertaining to Plaintiffs' and Putative Class members' PII. Plaintiffs have no interests antagonistic to the interests of the other Putative Class members.

57. Plaintiffs will fairly and adequately represent and protect the interests of the Putative Class members.

58. Plaintiffs have retained competent counsel experienced in complex litigation and class actions (including class actions brought under the FCRA), who will vigorously and competently prosecute the claims Plaintiffs and Putative Class members assert herein.

59. This class action provides a fair and efficient means for adjudicating the claims of Plaintiffs and Putative Class members for the following reasons:

a. Common questions of law and fact predominate over any question affecting any individual Putative Class member;

b. The prosecution of separate actions by individual Putative Class members would likely create a risk of inconsistent or varying adjudications with respect to individual class members, thereby establishing incompatible standards of conduct for the Defendants and would allow some Putative Class members' claims to adversely affect the ability of other members to protect their interests;

c. Plaintiffs anticipate no difficulty in the management of this litigation as a class action; and,

d. The above classes are readily definable. Prosecution as a class action will eliminate the possibility of repetitious litigation while also providing redress for claims that may be too small to support the expense of individual, complex litigation.

60. For these reasons, a class action is clearly superior to other available methods for the fair and efficient adjudication of this controversy. Certification, therefore, is appropriate under Rule 23(b)(1) or Rule 23(b)(3) of the Federal Rules of Civil Procedure.

VI.
CLAIMS FOR RELIEF

Count 1:
Willful violation of the Fair Credit Reporting Act
(On behalf of the Nationwide Class)

61. Plaintiffs allege and incorporate by reference all allegations asserted in the previous paragraphs.

62. The Putative Class members of the Nationwide Class, which includes the Plaintiffs, are consumers entitled to the protections of the Fair Credit Reporting Act, 15 U.S.C. § 1681a(c) ("FCRA").

63. Under the FCRA, a "consumer reporting agency" is defined as "any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties …" 15 U.S.C. § 1681a(f).

64. Equifax is a consumer reporting agency under the FCRA because, for monetary fees, it regularly engages in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties.

65. Equifax is also a CRA under 15 U.S.C. 1681a(p) because it is a "Consumer Reporting Agency that Compiles and Maintains Files on Consumers on a Nationwide Basis".

66. As a CRA, the FCRA requires Equifax to "maintain reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes listed under section 1681b of this title." 15 U.S.C. § 1681e(a).

67. Under the FCRA, a "consumer report" is defined as "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics,

or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for -- (A) credit . . . to be used primarily for personal, family, or household purposes; . . . or (C) any other purpose authorized under section 1681b of this title." 15 U.S.C. § 1681a(d)(1). The compromised data was a consumer report under the FCRA because it was a communication of information bearing on the Putative Class members' credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living used, or expected to be used or collected in whole or in part, for the purpose of serving as a factor in establishing the Class members' eligibility for credit.

68. As a CRA, Equifax may only furnish a consumer report under the limited circumstances set forth in 15 U.S.C. § 1681b, "and no other." 15 U.S.C. § 1681b(a).

69. None of the purposes listed under 15 U.S.C. § 1681b permit credit reporting agencies to furnish consumer reports to unauthorized or unknown entities, or computer hackers such as those who accessed Putative Class members' PII.

70. Equifax violated 15 U.S.C. § 1681b by furnishing consumer reports to unauthorized or unknown entities or computer hackers, as detailed above.

71. Equifax furnished Putative Class members' consumer reports by disclosing their consumer reports to unauthorized entities and computer hackers; allowing unauthorized entities and computer hackers to access their consumer reports; knowingly and/or recklessly failing to take security measures that would prevent unauthorized entities or computer hackers from accessing their consumer reports; and/or failing to take reasonable security measures that would prevent unauthorized entities or computer hackers from accessing their consumer reports.

72. The Federal Trade Commission ("FTC") has pursued enforcement actions against consumer reporting agencies under the FCRA for failing to "take adequate measures to fulfill their

obligations to protect information contained in consumer reports, as required by the" FCRA, in connection with data breaches.

73. Equifax willfully and / or recklessly violated §§ 1681b and 1681e(a) by providing impermissible access to consumer reports and by failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under section 1681b of the FCRA. The willful and reckless nature of Equifax's violations is supported by, among other things, former employees' admissions that Equifax's data security practices have deteriorated in recent years, and Equifax's numerous other data breaches in the past. Further, Equifax touts itself as an industry leader in breach prevention; thus, Equifax was well aware of the importance of the measures organizations should take to prevent data breaches, and willingly failed to take them.

74. Equifax also acted willfully and recklessly because it knew or should have known about its legal obligations regarding data security and data breaches under the FCRA. These obligations are well established in the plain language of the FCRA and in the promulgations of the Federal Trade Commission. *See, e.g.*, 55 Fed. Reg. 18804 (May 4, 1990), 1990 Commentary On The Fair Credit Reporting Act. 16 C.F.R. Part 600, Appendix to Part 600, Sec. 607 2E.

75. Equifax obtained or had available these and other substantial written materials that apprised it of Equifax's duties under the FCRA. There is no shortage of guidance, nor is there any defense available to Equifax that there existed only "a dearth of guidance" or that the FCRA and its regulations contained "less-than-pellucid statutory text" with regard to Equifax's willful violations of the FCRA. Any reasonable consumer reporting agency knows or should know about these requirements. Despite knowing these legal obligations, Equifax acted consciously in breaching known duties regarding data security and data breaches and depriving Plaintiffs and members of the Putative Classes of their rights under the FCRA.

76. In *Safeco Ins. Co.*, the Supreme Court held that willfulness under the FCRA requires a plaintiff to show that the defendant's conduct was intentional or reckless, where "reckless" consists of "action entailing an unjustifiably high risk of harm that is either known or so obvious that it should be known."[2]

77. Equifax engaged in conduct that was intentional or reckless, which provided a means for unauthorized intruders to obtain and misuse Plaintiffs' and Putative Class members' PII for no permissible purposes under the FCRA.

78. Plaintiffs and Putative Class members have been damaged by Equifax's willful or reckless failure to comply with the FCRA. Therefore, Plaintiffs and each of the Putative Class members are entitled to recover "any actual damages sustained by the consumer . . . or damages of not less than $100 and not more than $1,000." 15 U.S.C. § 1681n(a)(1)(A).

79. Plaintiffs and the Putative Class members are also entitled to punitive damages (which are most fitting in this case), costs of the action, and reasonable attorneys' fees under 15 U.S.C. § 1681n(a)(2) & (3).

Count 2:
Negligent violation of the Fair Credit Reporting Act
(On behalf of the Nationwide Class)

80. Plaintiffs allege and incorporate by reference all allegations asserted in the previous paragraphs.

81. Equifax was negligent in failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to only those purposes outlined in 15 U.S.C. § 1681b.

82. Equifax's negligent failure to maintain reasonable procedures is supported by, among other things, former employees' admissions that Equifax's data security practices have

[2] *Safeco Ins. Co. of Am. v. Burr*, 551 U.S. 47, 127 S. Ct. 2201, 167 L. Ed. 2d 1045, 2007 U.S. LEXIS 6963, 75 U.S.L.W. 4386, 20 A.L.R. Fed. 2d 803, 20 Fla. L. Weekly Fed. S 322.

deteriorated in recent years, and Equifax's numerous other data breaches in the past.

83. Further, as an enterprise claiming to be an industry leader in data breach prevention, Equifax was well aware of the importance of the measures organizations should take to prevent data breaches, yet failed to take them.

84. Equifax's negligent conduct provided a means for unauthorized intruders to obtain Plaintiffs' and Putative Class members' PII and consumer reports for no permissible purposes under the FCRA.

85. Plaintiffs and Putative Class members have been damaged by Equifax's negligent failure to comply with the FCRA.

86. Therefore, Plaintiffs and each of the Putative Class members are entitled to recover "any actual damages sustained by the consumer." 15 U.S.C. § 1681o(a)(1).

87. Plaintiffs and Putative Class members are also entitled to recover their costs of the action, as well as reasonable attorneys' fees. 15 U.S.C. § 1681o(a)(2).

Count 3:
Violation of State Data Breach Statutes and State Consumer Protection Statutes
(On behalf of Plaintiffs and the separate Statewide Sub-Classes)

88. Plaintiffs allege and incorporate by reference all allegations asserted in the previous paragraphs.

89. Legislatures in the states and jurisdictions listed below have enacted data breach statutes. These statutes generally require that any person or business conducting business within the state or U.S. Territory that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system to any resident of the state or U.S. Territory whose personal information was acquired by an unauthorized person, and further require that the disclosure of the breach be made in the most expedient time possible and without

unreasonable delay.

90. Defendants' data breach constitutes a breach of Equifax's security system within the meaning of the below state data breach statutes and the data breached is protected and covered by these data breach statutes.

91. Additionally, Plaintiffs' and Putative Class members' PII constitutes personal information under and subject to these state data breach statutes.

92. Defendants unreasonably delayed in informing the public, including Plaintiffs and members of each of the Statewide Sub-Classes, about the breach of security of Plaintiffs' and of members of each of the Statewide Sub-Classes' confidential and non-public personal information after Defendants knew or should have known that the data breach had occurred.

93. Defendants failed to disclose to Plaintiffs and members of each of the Statewide Sub-Classes without unreasonable delay and in the most expedient time possible, the breach of security of these individuals' personal and financial information when Defendants knew or reasonably believed such information had been compromised.

94. Plaintiffs and members of each of the Statewide Sub-Classes suffered concrete and tangible harm directly resulting from Defendants' failure to provide, and the delay in providing, Plaintiffs and the Statewide Sub-Class members with timely and accurate notice as required by the state data breach statutes. Plaintiffs and the Statewide Sub-Class members suffered the damages alleged above as a direct result of Equifax's delay in providing timely and accurate notice of the data breach.

95. Had Defendants given timely and accurate notice of the breach, Plaintiffs and the Statewide Sub-Class members would have been able to avoid and attempt to ameliorate / mitigate the damages and harm resulting in the unreasonable delay by Defendants in providing notice.

96. Defendants' failure to provide timely and accurate notice of the data breach violated the below state data breach statutes, and consumer protection statutes where applicable:

Data Breach Statutes:

a. Alaska Stat. Ann. § 45.48.010(a), *et seq*.;

b. Ark. Code Ann. § 4-110-105(a), *et seq*.;

c. Ariz. Rev. Stat. § 44-7501, *et seq*.;

d. Cal. Civ. Code § 1798.83(a), *et seq*.;

e. Colo. Rev. Stat. Ann § 6-1-716(2), *et seq*.;

f. Conn. Gen. Stat. Ann. § 36a-701b(b), *et seq*.;

g. Del. Code Ann. Tit. 6 § 12B-102(a), *et seq*.;

h. D.C. Code § 28-3852(a), *et seq*.;

i. Fla. Stat. Ann. § 501.171(4), *et seq*.;

j. Ga. Code Ann. § 10-1-912(a), *et seq*.;

k. Haw. Rev. Stat. § 487N-2(a), *et seq*.;

l. Idaho Code Ann. § 28-51-105(1), *et seq*.;

m. Ill. Comp. Stat. Ann. 530/10(a), *et seq*.;

n. Ind. Code §§ 4-1-11, *et seq*.

o. Iowa Code Ann. § 715C.2(1), *et seq*.;

p. Kan. Stat. Ann. § 50-7a02(a), *et seq*.;

q. Ky. Rev. Stat. Ann. § 365.732(2), *et seq*.;

r. La. Rev. Stat. Ann. § 51:3074(A), *et seq*.;

s. Me. Rev. Stat. tit. 10 § 1346 *et seq*.

t. Md. Code Ann., Commercial Law § 14-3504(b), *et seq*.;

u. Mass. Gen. Laws Ann. Ch. 93H § 3(a), *et seq*.;

v. Mich. Comp. Laws Ann. § 445.72(1), *et seq*.;

w. Minn. Stat. Ann. § 325E.61(1)(a), *et seq*.;

x. Miss. Code § 75-24-29;

y. Mo. Rev. Stat. § 407.1500;

z. Mont. Code Ann. § 30-14-1704(1), *et seq*.;

aa. Neb. Rev. Stat. Ann. § 87-803(1), *et seq*.;

bb. Nev. Rev. Stat. Ann. § 603A.220(1), *et seq*.;

cc. N.H. Rev. Stat. Ann. § 359-C:20(1)(a), *et seq*.;

dd. N.J. Stat. Ann. § 56:8-163(a), *et seq*.;

ee. 2017 H.B. 15, Chap. 36 (effective 6/16/2017, New Mexico);

ff. N.Y. Gen. Bus. Law §899-aa, *et seq*.;
N.Y. State Tech. Law 208, *et seq*.;

gg. N.C. Gen. Stat. Ann. § 75-65(a), *et seq*.;

hh. N.D. Cent. Code Ann. § 51-30-02, *et seq*.;

ii. Ohio Rev. Code §§ 1347.12, 1349.19, 1349.191, 1349.192;

jj. Okla. Stat. Ann. Tit. 24 § 163(A), *et seq*.;

kk. Oregon Rev. Stat. Ann. § 646A.604(1), *et seq*.;

ll. Pa. 73 Stat. § 2301, *et seq*.;

mm. R.I. Gen. Laws Ann. § 11-49.2-3(a), *et seq*.;

nn. S.C. Code Ann. § 39-1-90(A), *et seq*.;

oo. Tenn. Code Ann. § 47-18-2107(b), *et seq*.;

pp. Tex. Bus. & Com. Code Ann. § 521.053(b), *et seq*.,

qq. Utah Code Ann. § 13-44-202(1), *et seq*.;

rr. Va. Code. Ann. § 18.2-186.6(B), *et seq*.;

ss. Vt. Stat. tit. 9 §§ 2430, 2435;

tt. Wash. Rev. Code Ann. § 19.255.010(1), *et seq*.;

uu. W.V. Code §§ 46A-2A-101, *et seq*.;

vv. Wis. Stat. Ann. § 134.98(2), *et seq*.;

ww. Wyo. Stat. Ann. § 40-12-502(a), *et seq*.

xx. 9 GCA §§ 48-10, *et seq*.;

yy. 10 Laws of Puerto Rico §§ 4051, *et seq*.; and,

zz. V.I. Code tit. 14, §§ 2208, 2209 (U.S Virgin Islands).

State Consumer Protection Statutes:

a. The Alabama Deceptive Trade Practices Act, Ala. Code §§ 8-19-5(2), (3), (5), (7), and (27), *et seq*.;

b. The Arizona Consumer Fraud Act, A.R.S. § 44-1522;

c. The California Consumer Legal Remedies Act, Cal. Civ. Code § 1750, et seq., and the California Unfair Competition Law, Cal. Bus. and Prof. Code, § 17200, *et seq*.;

d. The Colorado Consumer Protection Act, Col. Rev. Stat. Ann. §§ 6-1-105(1)(b), (c), (e) and (g), *et seq*.;

e. The Connecticut Unfair Trade Practices Act, Conn. Gen. Stat. § 42-110(b), *et seq*.;

f. The Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. Ann. § 501.204(1), *et seq*.;

g. The Hawaii Deceptive Trade Practices Act, Haw. Rev. Stat. Ann. §§ 481A-3(a)(5), (7) and (12), et seq., and the Hawaii Consumer Protection Act, Haw. Rev. Stat. Ann. § 480-2(a), *et seq*.;

h. The Louisiana Unfair Trade Practices and Consumer Protection Law, La. Rev. Stat. Ann. § 51:1405(A), *et seq*.;

i. The Maryland Consumer Protection Act, Md. Code Commercial

Law, §§ 13-301(1) and (2)(i)-(ii), and (iv), (5)(i), and (9)(i), *et seq*.;

j. The Michigan Consumer Protection Act, M.C.P.L.A. §§445.903(1)(c)(e), (s) and (cc), *et seq*.;

k. The Mississippi Consumer Protect Act, Miss. Code Ann. §§ 75-24-5(1), (2)(b), (c), (e), and (g), *et seq*.;

l. The Missouri Merchandising Practices Act, Mo. Ann. Stat. §407.020(1), *et seq*.;

m. The Nebraska Consumer Protection Act, Neb. Rev. Stat. § 59-1602, and the Nebraska Uniform Deceptive Trade Practices Act, Neb. Rev. Stat. § 87-302(a)(5) and (7), *et seq*.;

n. The New Mexico Unfair Practices Act, N.M. Stat. Ann. §§ 57- 12-2(D)(5)(7) and (14) and 57-12-3, *et seq*.;

o. The New York Business Law, N.Y. Gen. Bus. Law § 349(a);

p. The North Carolina Unfair Trade Practices Act, N.C.G.S.A. § 75-1.1(a), *et seq*.;

q. The Ohio Consumer Sales Practices Act, Ohio Rev. Code Ann. §§1345.02(A) and (B)(1) and (2), *et seq*.;

r. The Oregon Unfair Trade Practices Act, Or. Rev. Stat. §§646.608(1)(e)(g) and (u), *et seq*.;

s. The Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 P.S. §§ 201-2(4)(v)(vii) and (xxi), and 201-3, *et seq*.;

t. The Tennessee Consumer Protection Act, Tenn. Code Ann. §§ 47-18-104(a), (b)(2), (3), (5), and (7), *et seq*.;

u. The Texas Deceptive Trade Practices Act, Tex. Bus. & Com. Code § 17.50(h);

v. The Utah Consumer Sales Practices Act, Utah Code Ann. §§ 13- 11-4(1), (2)(a), (b), and (i), *et seq*.;

w. The Washington Consumer Protection Act, Wash. Rev. Code §19.86.020, *et seq*.; and

x. The West Virginia Consumer Credit and Protection Act, W.V.A. Code § 46A-6-104, *et seq*.

97. Plaintiffs and members of each of the Statewide Sub-Classes seek all remedies available under their respective state data breach statutes and consumer protection statutes, including but not limited to (a) damages suffered by Plaintiff and Putative Class members as alleged above, to include restitution of the costs associated with the data breach; (b) disgorgement of all profits accruing to Equifax because of its deceptive trade practices, (c) equitable relief, including injunctive relief; (d) treble damages and (e) reasonable attorneys' fees and costs.

98. Plaintiffs bring this claim on behalf of themselves and the Putative Class members for the relief requested and to benefit the public interest. This claim supports the public interests in assuring that consumers are provided truthful, non-deceptive information about potential purchases and protecting members of the public from Equifax's Deceptive Trade Practices.

99. Equifax's wrongful conduct, including its deceptive trade practices has affected the public at large because a substantial percentage of the U.S. population has been affected by Equifax's conduct.

Count 4:
Negligence
(On behalf of Plaintiffs and the Nationwide Class, or, alternatively, Plaintiffs and the separate Statewide Sub-Classes)

100. Plaintiffs allege and incorporate by reference all allegations asserted in the previous paragraphs.

101. Equifax owed numerous legal duties to Plaintiffs and to members of the Nationwide Class, or, alternatively, members of the separate Statewide Sub-Classes (collectively, the "Class" as used in this Count). Equifax's duties included the following:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting PII in its possession;

b. to protect their PII using reasonable and adequate security procedures and systems that are compliant and consistent with industry-standard practices;

and

c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches, including promptly notifying Plaintiffs and Class members of the Equifax data breach.

102. Equifax owed a duty of care not to subject Plaintiffs, along with their PII, and Class members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices. Equifax solicited, gathered, and stored Plaintiffs' and Class members' PII for its commercial purposes.

103. Equifax knew, or should have known, of the risks inherent in collecting and storing PII and the importance of adequate security. Equifax received warnings from within and outside the company that hackers routinely attempted to access Personal Information without authorization. Equifax also knew about numerous, well-publicized data breaches by other companies.

104. Equifax knew, or should have known, that its computer systems did not adequately safeguard Plaintiffs' and Class members' PII.

105. Because Equifax knew that a breach of its systems would damage millions of consumers, including Plaintiffs and Class members, it had a duty to adequately protect their PII.

106. Equifax's own conduct also created a foreseeable risk of harm to Plaintiffs and Class members and their PII. Equifax's misconduct included failing to: (1) secure its point-of-sale systems, despite knowing their vulnerabilities, (2) comply with industry standard security practices, (3) employ adequate network segmentation, (4) implement adequate system and event monitoring, and (5) implement the systems, policies, and procedures necessary to prevent this type of data breach.

107. Equifax also had independent duties under state laws that required Equifax to reasonably safeguard Plaintiffs' and Class members' PII and promptly notify them about the data breach.

108. Equifax breached the duties it owed to Plaintiffs and Class members in numerous ways, including:

a. by creating a foreseeable risk of harm through the misconduct previously described;

b. by failing to implement adequate security systems, protocols and practices sufficient to protect their PII both before and after learning of the data breach;

c. by failing to comply with the minimum industry data security standards, during the period of the data breach; and

d. by failing to timely and accurately disclose that their PII had been improperly acquired or accessed.

109. But for Equifax's wrongful and negligent breach of the duties it owed Plaintiffs and Class members, their personal and financial information either would not have been compromised or they would have been able to prevent some or all of their damages.

110. The injury and harm that Plaintiffs and Class members suffered (as alleged above) was the direct and proximate result of Equifax's negligent conduct. Accordingly, Plaintiffs and the Class have suffered injury and are entitled to damages in an amount to be proven at trial.

Count 5:
Unjust Enrichment
(On behalf of Plaintiffs and the Nationwide Class, or, alternatively, Plaintiffs and the separate Statewide Sub-Classes)

111. Plaintiffs allege and incorporate by reference all allegations asserted in the previous paragraphs.

112. Plaintiffs and members of the Nationwide class or, alternatively, members of the

separate Statewide Sub-Classes (collectively, the "Class" as used in this Count), conferred a benefit on Equifax.

113. Specifically, they provided Equifax with (or otherwise allowed Equifax the use of) their PII in exchange for credit reports.

114. In exchange, Plaintiffs and Class members should have been protected by having Equifax process and store their PII using adequate data security.

115. Equifax knew that Plaintiffs and the Class members conferred a benefit on Equifax.

116. Equifax profited from using their PII for its own business purposes.

117. Equifax failed to secure the Plaintiffs' and Class members' PII, and, therefore, did not safeguard the benefit the Plaintiffs and Class members provided.

118. Equifax acquired the PII through inequitable means because it failed to disclose the inadequate security practices previously alleged.

119. Had Plaintiffs and Class members known that Equifax would not secure their PII using adequate security, they would not have furnished their PII (or allowed their PII to be furnished) to Equifax.

120. Plaintiffs and the Class have no adequate remedy at law.

121. Under the circumstances, it would be unjust for Equifax to be permitted to retain any of the benefits that Plaintiffs and Class members of the Class conferred on it.

122. Equifax should be compelled to disgorge into a common fund or constructive trust for the benefit of Plaintiffs and Class members proceeds that it unjustly received from them or as a result of receiving their data. In the alternative, Equifax should be compelled to refund any amounts that Plaintiffs and the Class may have paid.

VII.
DEMAND FOR JURY TRIAL

123. Pursuant to Fed. R. Civ. P. 38(b), Plaintiffs and members of the Putative Classes herein make formal demand for a trial by jury.

VIII.
PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and members of the Nationwide Class and Statewide Sub-Classes, pray for relief, seeking the Honorable Court to enter judgment that:

a. this action may proceed as a class action under Rule 23 of the Federal Rules of Civil Procedure;

b. certifies the Classes requested, appoints the Plaintiffs as class representatives of the applicable classes and the undersigned counsel for Plaintiffs as Class counsel;

c. declares that Equifax committed multiple, separate violations of the FCRA;

d. declares that Equifax acted willfully in knowing or reckless disregard of Plaintiffs' and all Putative Class members' rights and in disregard of its multiple obligations under the FCRA, and that such actions were objectively unreasonable;

e. awarding statutory and punitive damages as allowed by the FCRA;

f. declares that Equifax acted negligently, in disregard of Plaintiffs' and all Putative Class members' rights and in disregard of its multiple obligations under the FCRA;

g. awarding actual damages as allowed by the FCRA;

h. awarding reasonable attorneys' fees and costs as allowed by the FCRA;

i. on behalf of Plaintiffs and the Statewide Sub-Classes, enters an injunction against Equifax's Deceptive Trade Practices and requires Equifax to implement and maintain adequate security measures, including the measures specified above to ensure the protection of Plaintiffs' PII, which remains in the possession of Equifax;

j. on behalf of Plaintiffs and the Statewide Sub-Classes, awards appropriate equitable relief, including an injunction requiring Equifax to promptly notify all affected customers of future data breaches under respective states' data breach statutes;

k. orders Equifax to pay, in advance, the costs involved in notifying all class members of the Nationwide Class and of each Statewide Sub-Class about the judgment and in administering the claims process;

l. awards the Plaintiffs and all Class members appropriate monetary relief, including actual and statutory damages, restitution, and disgorgement;

m. awards Plaintiffs and all Classes' pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and

n. awards such other and further relief as this Court may deem just and proper.

Respectfully submitted,

ALI S. AHMED, P.C.

By: /s/ Salar Ali Ahmed
Salar Ali Ahmed
Federal Id. No. 32323
State Bar No. 24000342
One Arena Place
7322 Southwest Freeway, Suite 1920
Houston, Texas 77074
Telephone: (713) 223-1300
Facsimile: (713) 255-0013
Email: aahmedlaw@gmail.com

Attorney for Plaintiffs
and for Members of the Nationwide Class
and Statewide Sub-Classes